Lyddon Consulting Services response to consultation on Contingent Reimbursement model

November 14th 2018

Submitted by: Bob Lyddon, Director of Lyddon Consulting Services Ltd
(www.lyddonconsulting.com)

What is Lyddon Consulting?
A specialist consultancy in payments and electronic banking. We have recently acted as advisor regarding the UK payments landscape to a trade body representing UK Payment Institutions and to a major payments communications cooperative reviewing their UK market positioning. From 2003 to 2016 we were retained to run the central secretariat of IBOS Association, a global banking club arranging accounts and services for corporate customers, a central feature of which was the fulfilment of regulatory responsibilities for Customer Due Diligence.

What we have done in the field of Authorised Push Payments Fraud up to now:
We have carried out a major piece of research under the name of Project Carlton which examines the quantum and trajectory of APP Fraud, and the flaw within the Faster Payments system that enables it, which is replicated in the way banks process Internal Transfers.

We have recently made a submission into the Treasury Select Committee inquiry into Economic Crime on the subject, and two supplements as the nature of the plans for Confirmation of Payee and for the Contingent Reimbursement model have taken shape.

Confirmation of Payee and the Contingent Reimbursement model accept the current Faster Payments system as a given, and take no issue with its being replicated under New Payments Architecture.

This is one of five key points of perspective that we believe are missing behind the PSR's approach to APP Fraud, and which therefore invalidate the Contingent Reimbursement model at a conceptual level.

In addition there are five further, overarching points, and points of detail which we have addressed in our responses to the individual questions.

Contact details
Lyddon Consulting Services Ltd
14 Portsmouth Avenue
Thames Ditton KT7 0RT

07939 – 132341

bob@lyddonconsulting.com

Overarching points

a. Drafting

We find the code poorly drafted, with imprecise phraseology.

b. Scope

The scope is inadequate if it only reimburses non-personal customers that are microenterprises and charities. SMEs have been major losers from APP scams and they should be within scope. Indeed, we believe that it would be better to have a negative scope, classifying all victims as eligible unless they fall within given, limited categories.

c. Value Proposition for customers

The customer need not, and should not, be a party to this entire code. The customer requires a clear Value Proposition, as they have with the Direct Debit Guarantee. Any code should then be entirely between Payment Service Providers ("PSPs"), who should make clear to the customers whether they support the Value Proposition or not.

The scope of the code can be limited to those matters that need to be regulated between PSPs in order that the victim receives their reimbursement from their own PSP, whether or not it is that PSP or the beneficiary's PSP that is at fault.

d. Fault of beneficiary PSP

In our view the fault will lie with the beneficiary PSP unless they can prove otherwise, as they have (i) opened an account for a fraudster; and (ii) handled the proceeds of a crime.

e. No description of "As-Is" rights of the parties

The code should base itself upon where liability for different actions that contribute to the fraud lie now, with reference – inter alia - to:

- The 2017 Money Laundering Regulations, and particularly the obligations of the fraudster's PSP under Customer Due Diligence and their liability when they handle the proceeds of a crime;
- The 2017 Payment Services Regulations, and particularly how a victim of a fraud perpetrated via a "payment instrument" is covered and how that differs from the coverage for the victim of an APP scam;
- Terms of access to the Financial Ombudsman Service;
- The duty of care that a PSP owes to an account-holder;
- The duty of care that an account-holder owes to their PSP.

Five key points of perspective

Five key points invalidate the Contingent Reimbursement model draft code at a conceptual level.

I. Flaw in the Faster Payments system

There is a historic flaw within the Faster Payments system that enables APP Fraud. It derives from the original design of the system in around 2005. The Faster Payments design was based on the system for card payments at Point-of-Sale, because that was the only payment process in place at all of the largest UK banks at the time where such a bank could receive a message, process it and send a response in near-real-time.

The prime indication of Faster Payments being based on the POS chassis is its usage of the ISO8583 data standard, which is the cards standard. Vocalink was able to create the infrastructure for Faster Payments at short notice and without a build from scratch because it was already using the ISO8583 standard within its infrastructure for LINK.

There was at the time a process in operation within IBOS for the European member banks to receive a message, process it and send a response in near-real-time, but RBS was the only UK bank in IBOS, the infrastructure used by IBOS was and is SWIFTNet FIN (meaning that the messages are SWIFT MTs), and Vocalink was not involved. In consequence IBOS was not considered as a model upon which to base Faster Payments, notwithstanding the wide usage of SWIFTNet FIN and MT across the payments industry.

It must also be mentioned that Vocalink was able to re-use the BACS Sort Code Routing Tables to support Faster Payments because Vocalink runs the BACS infrastructure as well, and it is not coincidental that the field lengths in Faster Payments for the beneficiary name (even though it is not processed and checked at the beneficiary bank) and for the reference are limited to 18 characters, because the implementation of ISO8583 for Faster Payments reproduced limitations in the Standard18 data format used for BACS.

Faster Payments can be viewed as a system which made significant re-use of pre-existing elements of POS, LINK and BACS.

The central flaw that came with using a pull payment chassis (POS) upon which to build a push payment service (Faster Payments) was the absence of a beneficiary name-check at the beneficiary PSP. This function is not needed in a pull payment model like POS: the beneficiary initiates the POS payment themselves at their terminal and they have set up the relationship with their acquirer so as to ensure the funds go into their own account.

The beneficiary has no need to capture their own name, and the payment message that results and which is sent to card issuer does not cause a name-check between the card details and the beneficiary, because the card is the card of the payer and does not contain the beneficiary name.

The ISO8583 message as used within a POS model, when used in the Faster Payments implementation, does not result in a name-check at the beneficiary PSP even though it is needed in a push payment model. The beneficiary name – even if it is input into a payment template by the payer – is not processed at the beneficiary PSP i.e. it is not checked to ensure coherence with the name on the account that is associated with the payment destination indicated by the Sort Code and Account Number.

Faster Payments should be fundamentally re-engineered to eliminate this flaw, but this is not foreseen in the New Payments Architecture project.

II. Failure of beneficiary PSP's Customer Due Diligence

The beneficiary PSP has opened an account into which the proceeds of the APP Fraud are received. This indicates a failure of the beneficiary PSP's Customer Due Diligence during the onboarding phase, for which the PSP's culpability is absolute. The PSP is an "obliged entity" and has specific responsibilities around customers for whom it opens accounts, and these responsibilities do not diminish because of how other market actors in a payment chain behave.

The victim of APP Fraud is not an "obliged entity", a fact which has major ramifications on liability but one which is notable by its absence in the draft code.

III. Beneficiary PSP commits Money Laundering if it receives, credits and pays the proceeds of a fraud

If a PSP receives, credits and then relays funds that turn out to have been part of a criminal wrong-doing on the part of the PSP's account-holder, the PSP has itself committed a Money Laundering offence. Again the commission of the offence is neither mitigated nor diminished by the behaviour of other actors in the payment chain.

IV. Poorer coverage for a consumer under APP Fraud than when they use a "payment instrument"

Where a customer has used a "payment instrument" to effect a payment, the 2017 Payment Services Regulations (transposing Payment Services Directive 2) protect the customer against fraud up to a high bar.

The bar is firstly that the burden of proof of wrongdoing is on the PSP, not on the customer. Secondly the PSP must prove that the mistake was due to gross negligence or similar on the customer's part. The protection for a customer should not be lower under APP Fraud. The CRM draft code, however, offers the customer a radically lower level of protection.

V. Too narrow definition of what constitutes a "payment instrument"

We have a definitional issue in what constitutes a "payment instrument" and is therefore eligible for the PSD2 level of protection. A prime example is where the PSP's method for its customers to authorise a push payment employs a "payment instrument" (a debit card) in combination with an authenticator (such as a Vasco Digipass device) that a customer might well understand also to be a "payment instrument". The customer for sure uses one "payment instrument" and in combination with another object that a Man on the Clapham Omnibus might reasonably consider also to be a "payment instrument".

But, when used in combination, the result does not rank as a "payment instrument" under the 2017 PSRs. It would require a change in legislation – but a worthwhile one – to enlarge the scope of the definition of a "payment instrument" in the 2017 PSRs to include the cards/devices/combinations used to authorise push payments, and to ensure that surrogates for these objects – like Memorable Information – do not fall outside the scope of legal coverage when – towards the PSP's computers – their impact is the same.

Since the European Banking Authority's Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication come into force in the UK in September 2019 and require at least 2-dimensional security on all electronic payments, there is a near-term opportunity to eliminate the security gap on push payments that makes customers liable to lose far more when they use a push payment mechanism than when they use a "payment instrument".

That is an opportunity in the short term, whereas in the medium term the priority should be to re-engineer Faster Payments so as to include the name-check and on every payment. Were that to be done, the Confirmation of Payee would occur as part of the processing of every payment, and there would be no need for it as a separate, "overlay" service.

It would also change the landscape in which the CRM code would operate, rendering it redundant in its current form.

The obligation to credit the correct beneficiary as named in the payer's payment order should already lie squarely with the beneficiary PSP. The risks should be the same as with a cheque that is crossed "Account payee".

It is the beneficiary PSP's risk if it credits the cheque to an account with different naming than what the payer has written in the payee line of a cheque; it should be the PSP's risk if they credit a push payment to an account named differently to the contents of the payee field in a Faster Payment.

The beneficiary PSP's options should be to credit the funds, or to return the payment (not to reject it, as they have received settled funds).

If the PSP credits the payment and it turns out to be part of a fraud in which the beneficiary is culpable, the PSP has handled the proceeds of crime, which is money laundering. That offence would bring certain sanctions down upon it which, hopefully, would include reimbursement of the funds to the payer.

The PSP will also have failed in its Customer Due Diligence under the Money Laundering Regulations, having opened an account for a criminal in the first place. This is an absolute failing, in that the onboarding process must filter out actual or potential criminals such that, if one slips through the net, the PSP is liable for everything that stems from their own offence – and it is an offence, not just a failing.

Once again that offence would bring certain sanctions down upon the PSP which, hopefully, would include reimbursement of the funds.

The responsibilities of the beneficiary PSP under Anti-Money Laundering/Countering the Financing of Terrorism regulations are absolute in almost all cases, and do not diminish depending upon the behaviour of other parties. Inexplicably this basic rule-of-the-road is lost in the CRM draft code.

This has the effect of overlooking the rights of customers that derive, as third-party rights, from the obligations imposed on PSPs as "obliged entities" under AML/CFT legislation.

The deviation from this rule-of-the-road is exemplified by the CRM draft code containing fourteen instances of the word "reasonable". When applied to actions a PSP may have taken, the impact of the insertion of a test of reasonableness has the effect transferring risk away from the PSP and on to the payer.

In our experience (from IBOS) there is only one instance in AML/CFT regulations where the concept of reasonableness comes into play in a material way, and it is in putting a limitation on the enquiries that a PSP might have to undertake to establish the Ultimate Beneficial Ownership of a non-personal legal entity that is applying for an account. This is test is laid out in article 13.1.b of the 4th EU AML Directive.

The fourteen instances of the use of the word "reasonable" in the draft code are in GF.1.a, GF.3.a, SF1, SF1.2, SF1.2.a, SF1.3.a, SF1.5.a, SF2, SF2.1, SF2.3, SF2.5, R2.1.d, R2.3 and R4. This is in a document of 12 pages.

By contrast the 4th EU AML Directive is 45 pages long and only contains three other instances of the word "reasonable" beyond where it deals with Ultimate Beneficial Ownership:

1. Article 21, regarding who is the beneficiary of an insurance policy;
2. Article 33.1.b where an obliged entity has to inform the local Financial Intelligence Unit if they have reasonable grounds for suspecting that funds derive from criminal activity;
3. Article 60, to do with the postponement of publication of specific names involved in an AML lapse for a "reasonable" period of time.

It can be seen, then, that a test of reasonableness – which in the best of circumstances will involve a measure of subjective judgment – appears in the draft code far more often, and in connection to far more central points, than it appears in the 4th EU AML Directive, of which the 2017 Money Laundering Regulations are the UK's transposition.

Where any degree of subjective judgment comes into play, it should go without saying that this judgment should be exercised by a court of law, tribunal, the FOS or similar and not by the PSPs involved in the case.

Measured against the points listed above, the proposed CRM code does not do justice to those current rights of a customer that derive from the laws binding upon a PSP. The draft code muddies the waters for the customer, when it should make them as clear as they are under, for example, the Direct Debit Guarantee.

Given that the customer's rights in law are actually better than the CRM code, all the code can serve to do is to both waste time and to give the PSPs greater apparent rights against their customer than they actually have.

The CRM code should not proceed.

Work should re-start based on:

- what the customer's rights in law are;
- what the PSPs' obligations in law;
- what rights the customer derives as a third-party beneficiary from the PSPs' obligations in law;
- what the flaw is in the Faster Payments system and remedying it;
- putting in place a code to govern the period between when the current Money Laundering Regulations came into force (26th June 2017) and when the flaw in Faster Payments is remedied, such that the customer is protected against APP Fraud during that period to the same level they would have been protected if the same payment had been carried out using a "payment instrument".

During this interim period, changes need to be put through to the 2017 Payment Services Regulations that work with the EBA Regulatory Technical Standards and re-define the devices and processes used to authorise a push payment – and their surrogates such as Memorable Information - as being covered by the term "payment instrument".

In addition, during this interim period, the responsibilities of PSPs under current Money Laundering Regulations need to be reinforced to them by their respective financial regulators - with a reciprocal assurance being delivered to customers from those same financial regulators - that the financial sanctions imposed on PSPs for (i) handling the proceeds of crime obtained via APP Fraud; and (ii) a failure of Customer Due Diligence in the onboarding phase, will deliver the amount of money needed to place the account of the victim of an APP Fraud in the same position as if the fraud had not taken place – the same yardstick as is used to protect a customer from fraud around usage of a "payment instrument".

Individual responses

Core questions

Q1 Do you agree with the standards set out in the Standards for Firms

#	Comment
3.27	There should be no incentives to PSPs for them to carry out basic functions properly, and to comply with applicable laws and regulations
3.28	Self-assessment has no role to play here. The firm cannot be permitted to act as judge and jury
3.29	No comment
3.30	The word "better" is misplaced as the current protection is zero. What is the standard of protection that is being aimed at? If it is lower than that which applies when a customer uses a "payment instrument", there needs to be a solid justification as to why
3.31	This is absolute hygiene factor and has no place in such a code, or is it the case that firms do not have staff training?
3.32	The presupposition of this clause is that blame can be attached to a customer for falling victim to fraud. The best way to avoid fraud is to have products and services that frustrate fraud, not to put emphasis on the customer helping themselves. The underlying assumption is that if the customer does not heed the warnings that they receive during their "payment journey", the legal responsibility for the results can be transferred onto the customer, which is wrong
3.33	Incentivisation should play no role. If firms have expertise and ability they should apply this to doing the beneficiary name-check and to not opening accounts for fraudsters
3.34	This will be impossible to police and will have the sole effect of frustrating customers in obtaining redress from their PSP
3.35	QED – the warnings will frustrate customers in obtaining redress. A code such as this should not be about legitimising PSPs transferring their risks onto their customers
3.36	No comment
3.37	These generalisations set no effective marker
3.38	What does "do more" mean? More than what? Who will police this?
3.39	CoP was originally billed as solving APP Fraud. This downgrading of expectations of CoP is incorrect
3.40	No comment
3.41	Pay.uk has issued a brochure showing that CoP will only be available when a payment is set up, not each time the template is used, so the statement "When a customer is in the process of making a payment" incorrectly renders the scope of CoP. Pay.uk has also stated that a pay-out under the CRM will only be made if (i) the customer has used CoP; and (ii) the customer has received the "green tick" outcome of the three possible ones. There really needs to be clarity on what the actual deal is with CoP and it is disappointing that there are differences between the CRM code wording and communications coming from Pay.uk
3.42	This paragraph is very unclear and needs to be unbundled into what this means for the customer and the firm

#	Comments on Q1 (continued)
3.43	This paragraph, together with the following two, should rather be aimed at ensuring the victim is reimbursed speedily unless there is prima facie evidence that the victim acted with gross negligence or similar (the conditions under which a PSP can refuse to reimburse a victim of a fraud deriving from the usage of a "payment instrument"). The current contents, and the "Best Practice Code", smack of procedures to bat away customer claims
3.44	See response above
3.45	See response above

Q2 We welcome views on whether the provision that firms can consider whether compliance would have helped prevent the APP scam may result in unintended consequences – for example, whether this may enable firms to avoid reimbursing eligible victims

All we can see here is an infrastructure to legitimise firms not paying out, and being able to avoid their responsibilities not to open accounts for fraudsters. An inter-PSP code is indeed required to govern which PSP pays the reimbursement, and how the beneficiary PSP reimburses the victim's PSP, absent prima facie evidence of gross negligence or similar. There can then be a clear Value Proposition to the customer that the PSP community will meet the damage caused by APP Fraud, and then individual PSPs and Pay.uk need to make the necessary arrangements to squeeze APP Fraud out of the system without inveigling the customer into joint responsibility for doing so.

Q3 We welcome views on how these provisions (R2(1)(a) and (b)) might apply in a scenario where none of the parties have met their levels of care.

The customer has no duty of care in law towards their PSP. It is the PSP entirely that has a duty of care towards their customer. Imposing a duty of care on the customer is wrong, when APP Fraud derives from two things (i) PSPs open bank accounts for fraudsters; and (ii) PSPs running an external payment system (Faster Payments) that has no name-check obligation at the beneficiary bank.

We would add to this the contention that PSPs run their internal transfer (the third type of transfer that the code is supposed to govern beyond Faster Payments and CHAPS) along the same principles as they interact with Faster Payments: crediting is based on Sort Code and Account Number alone.

Q4. Do you agree with the steps customers should take to protect themselves?

It is hard to disagree with the steps themselves, but we do disagree with the supposition that there should be a transfer of responsibility from PSPs to customers based on whether customers have followed these steps.

Q5 Do you agree with the suggested approach to customers vulnerable to APP scams? In particular, might there be unintended consequences to the approach? Are there sufficient incentives for firms to provide extra protections?

All customers are vulnerable to APP scams, as has been proved. If the issue was resolved properly there need be no extra measures for "vulnerable customers". Building in such measures is unfair to supposedly non-vulnerable customers, who are equally as vulnerable to APP scams.

Q6 Do you agree with the timeframe for notifying customers on the reimbursement decision?
We disagree with the contention that is an acceptable response to deny reimbursement other than where the PSP puts forward a prima facie case that the victim has acted with gross negligence or similar, an accusation which must be laid out in due bureaucratic form together with the process that the PSP intends to follow to prove their claim. As is normal in civil and criminal proceedings where the PSP is the plaintiff, they must set out their evidence in such a form that the victim's counsel can deal with the claim.

Access to Financial Ombudsman service – R4
There is no question relating to this section and we refer to point 3.77 where it is stated: "The steering group considers that a customer who is refused reimbursement by a firm or has any other related complaint about a firm should, where eligible, be able to challenge the outcome by going to the FOS in a timely manner and having FOS review the decision".

The FOS is a service available to customers without the say-so of this steering committee. The steering committee has no right to put inferred qualifications on a customer's access to the FOS with insertions such as "where eligible" and "in a timely manner". The customer can challenge anything within the FOS' scope, whether there is a CRM code in place or not.

Q7 Please provide feedback on the measures and tools in the Annex to the code, and whether there any other measures or tools that should be included?
The measures can be described as "hygiene factor", "nice to have", "motherhood-and-apple-pie", because they do not go to the heart of the issue for the customer, are in many cases irrelevant to the customer and, if they happen at all, should happen out of view of the customer, without their involvement, and as measures for the PSPs to undertake in order to resolve the APP scams issue for their customers.

Q8 Do you agree that all customers meeting their requisite level of care should be reimbursed, regardless of the actions of the firms involved?
We disagree that there should be a required level of care for customers at all: they should be reimbursed unless their PSP can prove gross negligence (same tests as in PSD2 regarding a "payment instrument")

Q9 Do you agree that the sending firm should administer any such reimbursement, but should not be directly liable for the cost of the refund if it has met its own standard of care?
Only the sending firm – the victim's PSP – can deal with the victim. Whether they have to meet the full cost of reimbursement or can obtain some reimbursement from the beneficiary's PSP is a matter that should be dealt with in the only code that is needed: the inter-PSP one to back up the "Value Proposition" to the customer.

Q10 What is your view on the merits of the funding options outlined in paragraph 4.6? What other funding options might the working group consider?
We disagree with all the funding options. Once the sending and receiving PSPs realise they are going to have to reimburse victims to the same standard as prevails in the cards world, the problem will be resolved.

Major banks in the UK will find themselves as often on the victim side as on the fraudster side. Since they can be expected to adopt the Transaction Risk Analytics approach to complying with the European Banking Authority's Regulatory Technical Standards on Strong Customer Authentication and Common and Secure Communication, they will find themselves in a far better position to identify and reduce fraud themselves, without any actions on the part of their legitimate customers.

The remaining loophole will then be the lack of name-check in the processes for both Faster Payments and Internal Transfers: if APP scams were to be reimbursable in full other than in case of gross negligence or similar, the amount that PSPs would be looking at losing over a 5-year period – given the current quantum and trajectory of APP fraud – provides the business case for investing in eliminating the underlying problems.

We repeat – if PSPs are in a position where they will be reimbursing all APP frauds except where the victim has been grossly negligent, they will then find the money to take the necessary measures to control and eliminate this type of fraud.

Q11 How can firms and customers both demonstrate they have met the expectations and followed the standards in the code?
We consider this question as irrelevant given the views we have expressed above about the justifiability of the expectations and standards described.

Q12 Do you agree with the issues the evidential approach working group will consider?
As we have said that the code is unjustified in its present form, that the responsibilities of victim and PSP in law (including as third-party beneficiaries) should be the framework, as there is access to the FOS notwithstanding the existence of the code, we believe there is no need for the proposed task, and therefore no need for the evidential approach proposed nor indeed any other approach.

Q13 Do you recommend any other issues are considered by the evidential approach working group which are not set out above?
No, because the evidential approach is not required, as per our response to Q12 above.

Q14 How should vulnerability be evidenced in the APP scam assessment balancing customer privacy and care with the intent of evidential standards?
It should not be, for the reasons laid out in our response to Q5 above.

Q15 Please provide views on which body would be appropriate to govern the code.
If there were a code that met the requirements as we see them it would primarily be the FCA as main AML/CFT regulator of the UK's PSPs, supported by HMRC as AML/CFT regulator for a subset of PSPs. The main adjudication they would be called upon to make would be on whether the beneficiary PSP had:

I. adequately discharged its responsibility for Customer Due Diligence when onboarding the fraudster's account;
II. whether it had made itself guilty of money laundering by handling the proceeds of the scam.

The outcome would be the sharing of the reimbursement between the two PSPs (the only issue that needs addressing in any code) and the requisite penalties imposed on the PSPs for AML/CFT failings.

Q16 Do you have any feedback on how changes to the code should be made?
As our view is that the code is flawed in its suppositions, scope, intentions and content, we would reserve comment on this question until there was a draft code available that met with our concept.

Q17 Is a simple 50:50 apportionment for shared blame between firms appropriate? If not, what is a sensible alternative?
See response to question 15 above.

Q18 Would the ADR principles as adopted by Open Banking in section 7 of its Dispute Management System Code of Best Practice be an appropriate arbitration process for the code?
No, they are not needed if the code had the scope we have outlined above.

Q19 What issues or risks do we need to consider when designing a dispute mechanism?
None, as there is no need for one.

Additional Questions
Q20 What positive and/or negative impacts do you foresee for victims of APP scams as a result of the implementation of the code? How might the negative impacts be addressed?
Victims have more responsibilities placed upon them, possibly unknowingly. They will be gulled by PSPs into surrendering both rights under any code (which have no legal force anyway) and rights that exist in law. These impacts can be addressed by not proceeding with this code and instead by re-starting the project in the way we recommend in our introductory section.

Q21 What would be the positive and/or negative impact on firms (or other parties) as a result of the implementation of the code? How might the negative impacts be addressed?
PSPs will act as judge and jury over whether they have met the standards in the code, including applying their own subjective judgment as to whether their actions meet a test of reasonableness. This is unacceptable and will provide a bogus cloak of protection to PSPs against their customers. The code transfers risk from the PSP to the customer, without emphasizing the absolute responsibilities in law of PSPs in the AML/CFT area. These impacts can be addressed by not proceeding with this code and instead by re-starting the project in the way we recommend in our introductory section.

Q22 Are there any unintended consequences of the code, particularly those which may impact on consumers, which we should be aware of?
The transfer of risk from PSPs to customers.

Aside from what we have already said, there is another aspect that has aggravated APP fraud, and this is the progressive increase in the Faster Payments system limit from its initial £25,000 at launch to £250,000 now.

For a payment mechanism aimed at standing orders and at retail payments initiated from a mobile phone, tablet or PC, £25,000 was already too high. Now, at £250,000, it is in effect a High-Value Payment System and with the name-check defect.

Whilst it is the Faster Payments scheme company that has to propose any increase in the system limit to the Bank of England so as to be granted the Bank of England's non-objection, the increases have been driven as much by the Bank of England's policy of driving "non-systemically-important" payments off the CHAPS system, as by Faster Payments' desire to increase its payment volumes.

When CHAPS had its outage in October 2014 it came to light that the Bank of England had separate processes for "systemically-important" payments and "non-systemically-important" ones. We feel that we can say with assurance that customers were unaware of there being a process where PSPs submitting payments into CHAPS would decide which CHAPS function was to be invoked.

The Bank of England's defence that it is the submitting banks who decide whether a payment is systemically-important or not is invalid, because there is a financial incentive to submitting PSPs to classify payments as non-systemically-important, and because no benefit is offered to or accrues to the ordering party when their PSP decides that their payment is non-systemically-important. Ordering parties are only ever offered CHAPS as a unitary service, with a set fee per payment, and are not given a choice between the two modes of processing at the Bank of England, or a differential price.

On 20th October 2014 all systemically-important payments were processed, but non-systemically-important ones were not, and were held over until the following day even if some related to property completions. These customers had paid their £30-50 for a first-class payment, and then their payments were treated as second-class and they had to sleep in their cars overnight.

The Bank of England's contribution to APP fraud through their pusillanimous policy of pushing "non-systemically-important" payments off CHAPS and onto Faster Payments has not been surfaced anywhere in the PSR's work on the subject so we have taken the opportunity to record it here, for the customers who spent the night of 20th October 2014 in their cars, and were given no reimbursement of their £30-50 CHAPS fee.

Q23 How should the effectiveness of the code be measured?

Notwithstanding our views of the code in its current form, the yardsticks are simple:

- The average loss on an APP scam should be £300, the same amount as the average loss on card fraud;
- 60% of APP scams should be prevented by PSPs, without any action by the customer, the same percentage of fraud losses that are prevented in the cards world before they impact a victim;
- All APP scam victims should be reimbursed in full within 15 days by their PSP, unless their PSP can make a prima facie case of gross negligence or similar;
- A name-check is done at the beneficiary bank on all Faster Payments and Internal Transfers, and the risk of crediting for the beneficiary PSP is the same as crediting a cheque.

BL/14.11.18